Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)
Bundesamt für Cybersicherheit (BACS)

# Erläuterungen zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)

Mai 2024

# Inhaltsverzeichnis

# 1 Kontext

Der Bundesrat erteilte dem Eidgenössischen Finanzdepartement (EFD) am 11. Dezember 2020 den Auftrag, die Rechtsgrundlagen für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu erstellen. Sodann verabschiedete der Bundesrat am 2. Dezember 2022 den Entwurf über diese Rechtsgrundlagen und die Botschaft zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020[1] zuhanden des Parlaments. In der Folge hiess das Parlament die Änderungen des ISG am 29. September 2023 gut[2]; die Referendumsfrist verstrich am 18. Januar 2024 unbenutzt.

Der vorliegende Verordnungsentwurf enthält einerseits die Ausführungsbestimmungen zum 5. Kapitel des revidierten ISG über die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Andererseits werden auch organisationale Aspekte im Zusammenhang mit der Cybersicherheit geregelt. Die Verordnung soll zusammen mit dem revidierten 5. Kapitel des ISG auf den 1. Januar 2025 in Kraft treten.

Das Informationssicherheitsgesetz ist – ohne das oben erwähnte revidierte 5. Kapitel über die Aufgaben des neu geschaffenen Bundesamtes für Cybersicherheit (BACS) und die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen – bereits am 1. Januar 2024 in Kraft getreten. Auf diesen Zeitpunkt wurde zudem die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020[3] ausser Kraft gesetzt.[4] Die darin enthaltenen Bestimmungen wurden teilweise in das revidierte ISG überführt (insbesondere Begriffsdefinitionen). Jene Bestimmungen, welche in der CyRV die Informatiksicherheit des Bundes regelten, wurden in die Verordnung über die Informationssicherheit in der Bundesverwaltung (Informationssicherheitsverordnung, ISV)[5] übernommen. Die in der CyRV definierten Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC) – insbesondere dessen Aufgaben gegenüber der Wirtschaft und der Bevölkerung – werden nicht in der ISV geregelt, da sie mit der Revision des ISG eine neue gesetzliche Grundlage erhalten hat. Zudem wurde am 1. Januar 2024 das NCSC in das BACS im Eidgenössischen Department für Verteidigung, Bevölkerungsschutz und Sport (VBS) überführt. Aus diesem Grund finden sich daher organisationale Bestimmungen zum BACS in Art. 15*a* Abs. 1 und Abs. 2 Bst. a–g OV-VBS[6].

Die Aufgaben des BACS werden in der vorliegenden Verordnung – zusammen mit der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen – präzisiert und konkreter umschrieben. Die künftige Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) regelt somit in Ergänzung zur ISV die Aufgaben des BACS und die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Sie regelt daher schwergewichtig das Verhältnis zwischen dem BACS und Adressaten ausserhalb der Bundesverwaltung, während die ISV die Aufgaben und Zuständigkeiten für die Informationssicherheit innerhalb der Bundesverwaltung definiert.

---

1 SR 128
2 BBl 2023 2296
3 SR 120.73
4 AS 2023 735 (Anhang 2 Ziff. I).
5 SR 128.1
6 SR 172.214.1

# 2 Erläuterungen zu den einzelnen Bestimmungen

## 1. Abschnitt: Gegenstand

### Art. 1

Diese Bestimmung stützt sich auf die gesetzlichen Grundlagen im «5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen» des Informationssicherheitsgesetzes (Art. *73a* ff. ISG) und orientiert sich auch an Art. 15*a* Abs. 1 und Abs. 2 Bst. a–g OV-VBS.

*Artikel 1* umschreibt den Regelungsgegenstand der Verordnung und gibt mit den Bst. a–d die Struktur der Verordnung wieder, welche auch jeweils den Überschriften der jeweiligen Abschnitte entspricht:

*Bst. a:* *Nationale Cyberstrategie und deren Steuerungsausschuss*

Die Verordnung legt in den Artikeln 2–5 fest, dass der Bund in Abstimmung mit den Kantonen eine Nationale Cyberstrategie (NCS) definiert und einen Steuerungsausschuss (StA NCS) für deren Umsetzung einsetzt, wie dieser sich zusammensetzt, organisiert ist und welche Aufgaben diesem zukommen.

*Bst. b:* *Aufgaben des BACS*

Diese Verordnung regelt ergänzend in den Artikeln 6–10 die Aufgaben des BACS gemäss Art. 73*a* Abs. 2 ISG. Bis Ende 2023 waren die Aufgaben des NCSC, der Vorgängerorganisation des BACS, in der aufgehobenen CyRV geregelt. Mit der Ergänzungsrevision des ISG wurden diese Aufgaben in ein hierarchisch übergeordnetes formelles Gesetz übernommen.

*Bst. c:* *Informationsaustausch des BACS mit Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen*

Diese Verordnung regelt in den Artikeln 11–15 den Informationsaustausch zwischen dem BACS und den Behörden und Organisationen zum Schutz vor Cybervorfällen und Cyberbedrohungen über aktuelle Vorfälle, Bedrohungen und Angriffe im Bereich der Cybersicherheit. Es werden hierbei die Vorgaben, die Zuständigkeiten und Verantwortlichkeiten sowohl für das Kommunikationssystem für den sicheren Informationsaustausch als auch für das Informationssystem für den automatischen Austausch festgelegt, um sicherzustellen, dass relevante Informationen schnell und effektiv an die richtigen Stellen weitergeleitet werden können.

*Bst. d:* *Meldepflicht für Cyberangriffe*

In der Vernehmlassung zur Ergänzungsrevision des ISG wurde wiederholt gefordert, dass die Bestimmungen zur Meldepflicht bei Cyberangriffen auf kritische Infrastrukturen auf Verordnungsstufe konkretisiert werden sollen. Diesem Anliegen, das bereits in der Botschaft zur Änderung des Informationssicherheitsgesetzes[7] mehrfach erwähnt

[7] Botschaft vom 2. Dezember 2022 zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), BBl 2023 84.

wurde, soll mit den Artikeln 16–21 in der vorliegenden Verordnung Rechnung getragen werden. So werden insbesondere die Details der Meldepflicht geregelt, d.h. welche Behörden und Organisationen von der Meldepflicht ausgenommen sind, welche Cyberangriffe gemeldet werden müssen, was der Inhalt und der Umfang der Meldungen und der Ablauf des Meldeprozesses ist.

Erwähnenswert mit Blick auf die in diesem Artikel enthaltene abschliessende Aufzählung des Regelungsgegenstandes ist, dass sämtliche Vorgaben zur Cybersicherheit der Bundesverwaltung, die Zuständigkeiten und Aufgaben der Fachstelle des Bundes für Informationssicherheit und die sich daraus ergebenden Schnittstellen zu den Aufgaben des BACS in der ISV geregelt werden.

Ebenfalls nicht von der Cybersicherheitsverordnung werden die Massnahmen der Cyberverteidigung geregelt. Letztere betreffen die militärischen und nachrichtendienstlichen Massnahmen und umfassen insbesondere die in Art. 37 des Nachrichtendienstgesetzes[8] vorgesehenen aktiven Massnahmen zur Störung und Verlangsamung von Cyberangriffen. Sie betreffen auch die Massnahmen der Armee zur Gewährleistung ihrer Einsatzbereitschaft in allen Lagen und zur Bereitstellung von Fähigkeiten zur subsidiären Unterstützung der zivilen Behörden. Diese Massnahmen sind im Nachrichtendienstgesetz[9] und im Militärgesetz[10] sowie in den dazugehörigen Verordnungen geregelt.

## 2. Abschnitt: Nationale Cyberstrategie und Steuerungsausschuss

### Art. 2 Nationale Cyberstrategie

Die Bestimmungen zur nationalen Cyberstrategie waren bis Ende 2023 in Art. 5 der aufgehobenen CyRV geregelt. Der vorliegende Artikel knüpft an die damalige Regelung an und verpflichtet den Bundesrat, die Ziele und Massnahmen im Bereich des Schutzes vor Cyberrisiken in der Nationalen Cyberstrategie (NCS) festzulegen. Innerhalb der Bundesverwaltung ist gemäss Art. 15*a* Abs. 2 Bst. g OV-VBS das BACS zuständig, die NCS für den Bundesrat zu erarbeiten und deren Umsetzung zu koordinieren.

Die NCS bildet gemäss *Absatz 1* den strategischen Rahmen für die Prävention im Bereich der Cybersicherheit, der Früherkennung von Cyberbedrohungen, die Reaktionsmöglichkeiten und der Resilienz bei Vorfällen zum Schutz des Landes vor Cybervorfällen und Cyberbedrohungen. Dies bedeutet, dass die NCS einen umfassenden Ansatz zur Bewältigung von Cybervorfällen und Cyberbedrohungen verfolgt, der verschiedene Aspekte der Cybersicherheit umfasst:

– *Prävention im Bereich der Cybersicherheit*: Die Prävention bezieht sich auf Massnahmen, die ergriffen werden, um potenzielle Schwachstellen und Angriffsmethoden zu identifizieren und zu minimieren. Dies kann durch die Imple-

8 SR 121
9 Bundesgesetz über den Nachrichtendienst (NDG: SR 121).
10 Bundesgesetz über die Armee und die Militärverwaltung (MG: SR 510.10).

mentierung von Sicherheitsrichtlinien, Schulungen für Mitarbeiter, Sicherheitsaudits und den Einsatz von Sicherheitstechnologien geschehen.

- *Früherkennung von Cyberbedrohungen*: Die Früherkennung von Cyberbedrohungen beinhaltet die Fähigkeit, Anzeichen von Cybervorfällen und Cyberbedrohungen frühzeitig zu erkennen. Dies beinhaltet die Kontrolle von Netzwerken und Systemen auf verdächtige Aktivitäten und die Implementierung von Technologien zur Erkennung von Vorfällen und Bedrohungen.

- *Reaktionsmöglichkeiten bei Vorfällen*: Reaktionsmöglichkeiten bei Vorfällen bezieht sich auf die Fähigkeit, angemessen auf Cybervorfälle sowie Cyberbedrohungen zu reagieren, sobald diese erkannt werden. Dies kann die Aktivierung des Computer Emergency Response Teams (CERT), die Einleitung von Gegenmassahmen und die Zusammenarbeit mit anderen Behörden oder Organisationen zur Bewältigung des Vorfalls oder der Bedrohung umfassen.

- *Resilienz bei Vorfällen*: Resilienz bezieht sich mitunter auf die Geschwindigkeit, mit der sich ein System nach einem Cyberangriff wiederherstellen kann. Dies umfasst beispielsweise die Implementierung von Backup-Systemen, Notfallplänen und anderen Massnahmen zur Minimierung der Auswirkungen eines Angriffs.

- *Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität*: Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftätern und Straftäterinnen neuartige Möglichkeiten mit grossem Schadenspotenzial für Gesellschaft und Wirtschaft. Cyberkriminalität überschreitet territoriale Grenzen, und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Je stärker die digitale Vernetzung ist, desto grösser wird die Gefahr, dass Cybervorfälle zwar in der virtuellen Welt beginnen, aber ihre schädigende Wirkung in der realen Welt entfalten. Vor dem Hintergrund dieser Entwicklung ist es wichtig, gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern die Interoperabilität und Reaktionsfähigkeit weiter zu verbessern sowie die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne dabei die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben.

Die NCS legt den Rahmen für diese verschiedenen Aspekte fest und koordiniert die Anstrengungen auf nationaler Ebene gemäss *Absatz 2* in enger Abstimmung mit den Kantonen. Mit einer umfassenden Strategie soll sichergestellt werden, dass die Schweiz gesamthaft besser gegen Cybervorfälle und Cyberbedrohungen geschützt ist und effektiv auf diese reagieren kann.

## Art. 3 Einsetzung und Organisation des StA NCS

Die Funktion und Zusammensetzung des Steuerungsausschusses der Nationale Cyberstrategie (StA NCS) war bis Ende 2023 in Art. 9 der aufgehobenen CyRV geregelt.

*Absatz 1: Einsetzung des StA NCS durch den Bundesrat*

*Absatz 1* legt fest, dass der StA NCS vom Bundesrat eingesetzt wird, um dem Gremium das nötige politische Gewicht zu verleihen. Es steuert und überwacht die Umsetzung der NCS und koordiniert die Massnahmen zur Stärkung der Cybersicherheit auf nationaler Ebene. Der StA NCS spielt eine wichtige Rolle bei der Schaffung eines ganzheitlichen Ansatzes zur Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz. Durch die Koordination und Überwachung der Massnahmen zur Umsetzung der NCS trägt der Steuerungsausschuss dazu bei, dass die Schweiz besser vor Cybervorfällen und Cyberbedrohungen geschützt ist und effektiv auf aktuelle Gefahren reagieren kann.

*Absatz 2: Organisation des StA NCS*

Das BACS stellt gemäss *Absatz 2* das Sekretariat des StA NCS. Damit hat es eine administrative sowie organisatorische Unterstützungsfunktion gegenüber dem Ausschuss und hilft bei der Koordination der Ausschussaktivitäten, der Vorbereitung von Sitzungen, der Erstellung von Protokollen und Berichten sowie bei der Kommunikation mit den Mitgliedern und anderen relevanten Akteuren. Durch die Bereitstellung des Sekretariats ermöglicht das BACS dem StA NCS effektiv zu arbeiten und unterstützt damit zusätzlich die Umsetzung der NCS. Dabei bringt das BACS seine Fachkenntnisse im Bereich der Cybersicherheit ein und unterstützt eine effiziente Zusammenarbeit zwischen den verschiedenen Mitgliedern des Ausschusses.

## Art. 4 Zusammensetzung des StA NCS

*Absatz 1: Mitgliederkreis des StA NCS*

Bei der Zusammensetzung des StA NCS ist zu beachten, dass es sich bei der NCS um eine nationale Strategie handelt, die sich nicht auf die Aktivitäten des Bundes beschränkt. Deshalb ist es wichtig, dass auch die Kantone, die Wirtschaft, die Gesellschaft und die Hochschulen im StA NCS vertreten sind. Die Zusammensetzung des StA NCS widerspiegelt die Notwendigkeit, dass die Umsetzung der NCS eine breite und vielfältige Beteiligung erfordert:

- Die *Vertretungen der Departemente und der Bundeskanzlei* bringen die Perspektive der Bundesverwaltung ein und diese sind für die Koordination und Umsetzung von Massnahmen auf Bundesebene verantwortlich.

- Die *Vertretungen der Kantone* stellen sicher, dass die Interessen und Bedürfnisse der Kantone in Bezug auf Cybersicherheit berücksichtigt werden. Da viele Aspekte der Cybersicherheit auch auf kantonaler Ebene relevant sind, ist der Einbezug der Kantone für eine effektive nationale Strategie wichtig.

- Die *Vertretungen der Wirtschaft, Gesellschaft und Hochschulen* bringen verschiedene Fachkenntnisse und Perspektiven ein. Die Wirtschaft ist oft ein Hauptziel von Cybervorfällen und Cyberbedrohungen und kann wertvolle Einblicke in diese bieten. Die Gesellschaft repräsentiert die Interessen der Bürgerinnen und Bürger in Bezug auf die digitale Sicherheit und das Funktionieren

kritischer Infrastrukturen. Die Hochschulen können ihre Expertise in Forschung und Innovation im Bereich der Cybersicherheit einbringen.

Insgesamt ermöglicht diese breite Zusammensetzung des StA NCS eine umfassende Betrachtung verschiedener Aspekte der Cybersicherheit und fördert eine koordinierte Zusammenarbeit zwischen den verschiedenen Akteuren auf nationaler Ebene. Dies trägt zu einer effizienten Umsetzung der NCS und einem besseren Schutz der Schweiz vor Cybervorfällen und Cyberbedrohungen bei.

*Absatz 2 und 3: Wahl der Mitglieder des StA NCS sowie der vorsitzenden Person durch den Bundesrat*

Der Bundesrat bestimmt im Rhythmus von fünf Jahren die Mitglieder des StA NCS, mit Ausnahme der Vertreterinnen und Vertreter der Kantone, welche durch die Konferenz der Kantonsregierungen ausgewählt werden. Die regelmässige Ernennung von Mitgliedern im Rhythmus von fünf Jahren ermöglicht dem Bundesrat, sicherzustellen, dass der StA NCS mit aktuellen und kompetenten Vertretungen besetzt ist, die über das erforderliche Fachwissen und die notwendigen Fähigkeiten verfügen, um die NCS effektiv umzusetzen. Dies trägt zur Aktualität und Relevanz des Ausschusses bei. Die Ernennung der vorsitzenden Person aus den Vertretungen der Wirtschaft, der Gesellschaft oder der Hochschulen unterstreicht die Bedeutung einer ausgewogenen Führung des Ausschusses. So kann die vorsitzende Person eine breite Perspektive einbringen und sicherstellen, dass die Interessen verschiedener Sektoren angemessen berücksichtigt werden. Insgesamt ermöglicht diese Struktur eine kontinuierliche Anpassung an neue Entwicklungen im Bereich der Cybersicherheit und fördert eine ausgewogene Beteiligung verschiedener Interessengruppen an der Umsetzung der NCS. Dies trägt zu einer effizienten Umsetzung der NCS und einem besseren Schutz der Schweiz vor Cybervorfällen und Cyberbedrohungen bei.

## Art. 5 Aufgaben des StA NCS

Die in *Artikel 5* gemachte Auflistung der Aufgaben des StA NCS sind auf eine effektive Umsetzung und Überwachung der NCS ausgerichtet und beinhaltet was folgt:

- *Bst. a:* Die regelmässige Überprüfung der NCS im Mindestrhythmus von fünf Jahren ermöglicht es dem Ausschuss, sicherzustellen, dass die Strategie an aktuelle Entwicklungen und Bedrohungen angepasst und dementsprechend weiterentwickelt wird. Im Bedarfsfall werden seitens des Ausschusses konkrete Empfehlungen oder Pläne gemacht, die darauf abzielen, die bestehende NCS anzupassen.

- *Bst. b:* Die Festlegung von Prioritäten und Zeitplänen für die Umsetzung der Massnahmen stellen einen effektiven Einsatz der Ressourcen und die Erreichung der Ziele der Strategie sicher.

- *Bst. c:* Die laufende Beurteilung des Fortschritts bei der Umsetzung der Massnahmen ermöglicht es dem Ausschuss, Engpässe oder Probleme frühzeitig zu

erkennen, entsprechend zu reagieren und den Bundesrat und die Kantone über Verzögerungen zu informieren.

- *Bst. d:* Die Formulierung von Vorschlägen für ergänzende Massnahmen zuhanden des Bundesrates trägt dazu bei, dass Hindernisse schnell beseitigt werden können.

- *Bst. e:* Der jährliche Bericht über die Umsetzung der NCS stellt Transparenz sicher und ermöglicht es allen relevanten Akteuren, den Fortschritt zu verfolgen und gegebenenfalls Anpassungen vorzunehmen.

## 3. Abschnitt: Aufgaben des BACS

### Art. 6 Halterabfragen

Diese Bestimmung stützt sich auf Art. 73*a* Abs. 1 und 2 Bst. a sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

Die Aufgabe des BACS betreffend die Warnung der Öffentlichkeit wurde bis Ende 2023 in Art. 12 Abs. 1 Bst. h der aufgehobenen CyRV geregelt und ist seit dem 1. Januar 2024 in Art. *15a* Abs. 2 Bst. d und e OV-VBS aufgeführt.

Seit 2010 wird MELANI (Melde- und Analysestelle Informationssicherung), welche im Jahr 2020 vom NCSC und schliesslich seit Anfang dieses Jahres durch das BACS abgelöst wurde, vom Bundesamt für Kommunikation (BAKOM) als «eine zur Bekämpfung der Cyberkriminalität vom BAKOM anerkannte Stelle» gemäss Art. 15 Abs. 3 VID[11] betrachtet.[12] Da das BACS aber keine strafrechtlichen Kompetenzen oder Aufgaben hat, ist es nur indirekt mit der Cyberkriminalität befasst. Um die Zuständigkeit des BACS für die Abfrage von Kontaktangaben der Halter von Domain-Namen bei der Registerbetreiberin klarzustellen, wird diese Befugnis ausdrücklich in *Artikel 6* erwähnt (vgl. diesbezüglich Art. 28*e* Bst. b FMG und Art. 7 ff. VID).[13] Die Möglichkeit, Kontaktangaben von Haltern von Domain-Namen abzufragen, ermöglicht es dem BACS, beispielsweise im Falle von akuten Cyberbedrohungen oder Cyberangriffen schnell und gezielt potenziell betroffene Parteien zu warnen und sie gegebenenfalls bei der Umsetzung von Gegenmassnahmen zu unterstützen. Diese Befugnis ist ein wichtiges Instrument zur Bekämpfung von Cyberbedrohungen sowie -angriffen und zur Stärkung der Cybersicherheit in der Schweiz.

---

11 Verordnung vom 5. November 2014 über Internet-Domains (VID; SR 784.104.2).

12 Siehe hierzu die Webseite des BAKOM «Bekämpfung der Internetkriminalität» (zuletzt besucht 29. März 2024).

13 Das BAKOM hat der Stiftung SWITCH die Zuteilung bzw. Verwaltung der .ch-Domain-Namen übertragen (vgl. Art. 28*a* Abs. 1 Fernmeldegesetz vom 30. April 1997 [FMG; SR 784.10] und Art. 8 Abs. 2 i.V.m. Art. 33 VID vom 5. November 2014), die SWITCH in einer RDDS-Datenbank (WHOIS) verwaltet. Das BACS hat eine Vereinbarung mit SWITCH abgeschlossen, die die Bekanntgabe der Domainhalter in der RDDS-Datenbank (WHOIS) im Abrufverfahren über den RDAP-Zugang regelt.

## Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen

Diese Bestimmung stützt sich auf Art. 73*a* Abs. 1 und Abs. 2 Bst. a und e sowie Art. 74 Abs. 3 i.V.m. Art. 74*a* Abs. 3 ISG.

Die Aufgaben des nationalen Computer Emergency Response Team (CERT) war bis Ende 2023 in Art. 12 Abs. 1 Bst. c der aufgehobenen CyRV geregelt. Dieses wird ab 1. Januar 2024 in Art. *15a* Abs. 2 Bst. f OV-VBS aufgeführt.

*Absatz 1: Computer Emergency Response Team (CERT)*

Das BACS betreibt das nationale Computer Emergency Response Team (CERT), das eine zentrale Rolle bei der Bewältigung von Cybervorfällen und Cyberbedrohungen in der Schweiz spielt. Das CERT ist spezialisiert auf die technische Vorfallbewältigung, die Analyse von technischen Fragestellungen sowie Identifikation und der Einschätzung von Cyberbedrohungen aus technischer Sicht.

Kernelement der Analyse von technischen Fragestellungen ist der Abgleich von Daten aus Cyberangriffen und die Suche nach Anomalien (Bst. a). Dazu entwickelt das CERT eigene Analyseinstrumente und nutzt Analyseinstrumente Dritter. Es tauscht sich zudem eng mit Spezialistinnen und Spezialisten aus den Sicherheitsteams der Privatwirtschaft und anderer Länder aus.

Die Unterstützung des BACS bei der Bewältigung von Vorfällen besteht in der technischen Analyse des Angriffs (Bst. b). Diese hat zum Ziel, möglichst rasch zu verstehen, welche Angriffsmethoden die Angreifer nutzen, welche Methoden und Taktiken sie anwenden und welche Ziele sie verfolgen. Diese Erkenntnisse ermöglichen es, geeignete Gegenmassnahmen zu bestimmen und umzusetzen. Das BACS arbeitet dabei eng mit den betroffenen Behörden und Organisationen und ihren allfälligen Sicherheitsdiensten zusammen. Es hilft zudem bei der Koordination zwischen den an der technischen Bewältigung beteiligten Akteuren. Bei Bedarf kann es auch direkt vor Ort bei der betroffenen Behörde oder Organisation Unterstützung leisten. Die Unterstützung durch das BACS erfolgt im Sinne einer Soforthilfe im Notfall. Bei den nach der Vorfallbewältigung nötigen Arbeiten zur Wiederherstellung der Daten und Wiederaufbau der Systeme unterstützt das BACS nur beratend.

Das CERT unterstützt Behörden und Organisationen auch präventiv. Es analysiert laufend neue technische Bedrohungen und Angriffsmethoden und identifiziert geeignete Gegenmassnahmen (Bst. c). Die technischen Einschätzungen der Bedrohungslage erfordern eine Kombination aus automatisierten Tools zur Analyse von Cybervorfällen und Cyberbedrohungen, dem Informationsaustausch mit nationalen und internationalen Fachstellen sowie menschlicher Expertise zur Interpretation der Ergebnisse. Die kontinuierliche Wahrnehmung dieser Einschätzungen ermöglicht es, proaktiv auf Gefahren zu reagieren, Sicherheitslücken zu schliessen und ihre Verteidigungsstrategien anzupassen, um sich gegen aktuelle und zukünftige Cybervorfälle und Cyberbedrohungen zu schützen.

*Absatz 2: Resiliente Infrastruktur*

Das BACS betreibt eine resiliente Infrastruktur, die unabhängig von der restlichen Informatik des Bundes funktionieren muss. Dies bedeutet, dass das BACS ein Leistungserbringer für diese spezifische Infrastruktur ist und daher über spezielle technische Ressourcen und Systeme verfügt, um Cybervorfälle und Cyberbedrohungen zu analysieren.

Die Notwendigkeit einer unabhängigen Infrastruktur ergibt sich aus der Sensibilität und Dringlichkeit von Cybervorfällen und Cyberbedrohungen. Da das BACS die nationale Anlaufstelle für Cybersicherheit ist, muss es auch bei einer Beeinträchtigung der Bundesinformatik in der Lage sein, zuverlässig Cybervorfälle und Cyberbedrohungen zu analysieren.

Diese unabhängige und resiliente Infrastruktur ermöglicht es dem BACS, seine Aufgaben effektiv zu erfüllen und sicherzustellen, dass die Schweiz auf Cybervorfälle und Cyberbedrohungen angemessen reagieren kann.

## Art. 8 Priorisierung der Beratung und Unterstützung bei Cyberangriffen

Diese Bestimmung stützt sich auf Art. 74 Abs. 3 und Art. *74a* Abs. 3 ISG.

*Allgemeines:*

Art. 74 Abs. 3 ISG sieht vor, dass das BACS die Betreiberinnen von kritischen Infrastrukturen bei der Bewältigung von Cybervorfällen und Cyberbedrohungen sowie bei der Behebung von Schwachstellen beraten und unterstützen kann. Dies unter der Voraussetzung, dass die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist. Die Betroffenen entscheiden dabei selbst, ob sie die Unterstützung des BACS in Anspruch nehmen wollen.

Die Beratung und Unterstützung erfolgen hauptsächlich durch technische Analysen und Auskünfte zu technischen und organisatorischen Massnahmen. Durch die technischen Analysen soll die Ursache des Vorfalls identifiziert, das Ausmass der Kompromittierung verstanden und die potenziellen Schwachstellen bei den Informatikmitteln sowie dem Sicherheitssystem erkannt werden. Dies kann beispielsweise die Untersuchung von Systemprotokollen, Malware-Analysen sowie Auswertungen der Netzwerküberwachung umfassen. Neben den technischen Analysen bietet das BACS auch die Beratung zu organisatorischen Massnahmen an, um den Vorfall besser zu bewältigen. Da das BACS bei vielen Vorfällen involviert ist, kann es beispielsweise Hinweise geben, wie der Vorfall kommuniziert werden kann oder welche Notfallorganisation notwendig ist.

*Absatz 1: Priorisierung der Beratungs- und Unterstützungsleistungen*

Absatz 1 befasst sich mit der Situation, in der das BACS mit einer höheren Anzahl von Anfragen für Beratung und Unterstützung im Falle eines Cyberangriffs konfrontiert wird, als es mit seinen vorhandenen Personal- und technischen Ressourcen und Kapazitäten bewältigen kann. In solch einem Szenario behält sich das BACS das

Recht vor, Entscheidungen darüber zu treffen, welche Anfragen zuerst bearbeitet werden und wie umfangreich die Unterstützung ausfallen wird. In anderen weniger dringenden Fällen werden die Beratung sowie Unterstützung entsprechend zeitlich verzögert geleistet. Neben dem Zeitpunkt kann auch der Grad der zur Verfügung gestellten Hilfe variieren. Einige Fälle können eine vollständige Untersuchung und umfassende Unterstützung erfordern, während andere vielleicht nur eine grundlegende Beratung erhalten. Diese Bestimmung ermöglicht es dem BACS, in Zeiten hoher Auslastung strategische Entscheidungen darüber zu treffen, wie seine Ressourcen am besten eingesetzt werden können, um die grösstmögliche Hilfe zu leisten.

*Absatz 2: Priorisierung unter Berücksichtigung öffentlicher Interessen*

Das BACS unterstützt im Falle einer Vielzahl von zeitgleichen Cybervorfällen und Cyberbedrohungen vorrangig die meldepflichtigen Organisationen und Behörden, bei denen das Ereignis die grössten Auswirkungen auf die Sicherheit, die öffentliche Ordnung, das Wohlergehen der Bevölkerung oder das Funktionieren der Wirtschaft hat. Das bedeutet, dass das BACS seine Ressourcen und Unterstützung gezielt dort einsetzt, wo die Auswirkungen eines Ereignisses besonders gravierend sind. Dies kann beispielsweise bedeuten, dass kritische Infrastrukturen, Behördeneinrichtungen oder andere wichtige Organisationen priorisiert werden, um sicherzustellen, dass sie angemessen geschützt sind und im Falle eines Angriffs schnell Unterstützung erhalten. Durch diese Priorisierung kann das BACS sicherstellen, dass diejenigen Einrichtungen und Organisationen, die für das Funktionieren von Gesellschaft und Wirtschaft am wichtigsten sind, im Falle von Cybervorfällen und Cyberbedrohungen angemessen geschützt werden. Dies trägt dazu bei, die Resilienz und Stabilität des Landes im Falle eines grossflächigen Ereignisses, das viele Ziele in der Schweiz betrifft, zu gewährleisten.

## Art. 9 Koordinierte Offenlegung von Schwachstellen

Diese Bestimmung stützt sich auf Art. *73a* Abs. 2 Bst. c sowie auf Art. 73*b* Abs. 3 i.V.m. Art. 73*c* Abs. 2 ISG.

Die Aufgaben des BACS im Zusammenhang mit der Schwachstellenkoordination waren in der CyRV nicht explizit geregelt, sondern durch die allgemeinen Aufgaben des BACS abgedeckt, welche seit dem 1. Januar 2024 neu in Art. *15a* Abs. 2 Bst. b OV-VBS aufgeführt sind. Zudem ist seit dem 1. Januar 2024 eine Rechtsgrundlage für die Schwachstellensuche in der Informatikinfrastruktur der Bundesverwaltung und der Armee in Art. 43 Abs. 1 Bst. c ISV enthalten. Diese Bestimmung sieht vor, dass das BACS mitunter die Bundeskanzlei, die Generalsekretariate, Departemente und die Bundesämter über aktuelle Bedrohungen und Schwachstellen sowie über Risiken, die sie betreffen, informiert und bei Bedarf Massnahmen zur Risikominderung empfiehlt.

Die Wichtigkeit eines aktiven Schwachstellenmanagements und die Rolle des BACS bei der Suche und der koordinierten Offenlegung von Schwachstellen wird ausführli-

cher im Bericht des Bundesrats «Die Förderung des ethischen Hackings in der Schweiz»[14] beschrieben.

*Absatz 1: Koordiniert Offenlegung von Schwachstellen*

Die koordinierte Offenlegung von Schwachstellen ist ein wichtiger Bestandteil der globalen Cybersicherheitsbemühungen, da sie es ermöglicht, potenzielle Sicherheitslücken in IT-Systemen zu analysieren, zu bewerten und zu beheben, bevor sie von Angreifern ausgenutzt werden können. Der Prozess der koordinierten Offenlegung zielt darauf ab, eine möglichst hohe Transparenz über Schwachstellen zu ermöglichen, ohne Sicherheitsrisiken zu erzeugen. Kernelement des Prozesses ist, dass nach dem Finden einer Schwachstelle zunächst die Hersteller informiert werden. Mit diesen vereinbaren die Hacker eine Sperrfrist, innerhalb derer sie keine Informationen zur Schwachstelle öffentlich verbreiten. Dies gibt den Herstellern genügend Zeit, die Schwachstelle zu beheben, bevor sie öffentlich gemacht wird. Dieser Prozess ist international etabliert und wird beispielsweise auch in der EU durch die NIS-2-Richtlinie (Art. 12 und 13) vorgeschrieben.[15]

Die Regeln für die koordinierte Offenlegung von Schwachstellen sind in der ISO/IEC Norm 29147:2018-10 festgelegt.[16] Das BACS ist verpflichtet, gemeldete Schwachstellen gemäss den in dieser Norm festgelegten Regeln offenzulegen. Dies bedeutet, dass das BACS keine Schwachstellen geheim behält oder anderen Behörden weiterleitet, ohne die Hersteller zu informieren. Das BACS ist vielmehr verpflichtet, über den Prozess der koordinierten Offenlegung Massnahmen umzusetzen, die dazu führen, dass die Schwachstelle nicht mehr ausgenutzt werden kann.

Durch die Zusammenarbeit mit ausländischen und internationalen Fachstellen kann das BACS sicherstellen, dass Schwachstellen auf internationaler Ebene erkannt und behoben werden. Das BACS wurde im September 2021 von der US-Organisation MITRE als Fachstelle für Schwachstellen anerkannt und autorisiert, Schwachstellen gemäss dem Standard «Common Vulnerabilities and Exposure (CVE)» zur Kennzeichnung und Identifizierung eine CVE-Nummer zuzuweisen, damit bekannte Schwachstellen eine eindeutige Bezeichnung erhalten. Dies ermöglicht Sicherheitsexperten, Herstellern, Anwendern und Behörden, sich in einheitlicher Weise auf diese Schwachstelle zu beziehen. Durch die Verwendung von CVE-Nummern können Sicherheitslücken effektiver kommuniziert, dokumentiert und behoben werden. Die Verwendung eines standardisierten Namensschemas erleichtert auch die Zusammenarbeit zwischen den verschiedenen Akteuren im Bereich der Cybersicherheit und trägt dazu bei, die Transparenz und Effektivität bei der Behandlung von Sicherheitslücken zu verbessern.

---

[14] Vgl. hierzu: Bericht des Bundesrates vom 29. November 2023, Die Förderung des ethischen Hackings in der Schweiz, Bericht des Bundesrates in Erfüllung des Postulats 20.4594, Bellaiche, vom 17. Dezember 2020, Ziff. 4.2.4., S. 13 f.

[15] NIS-2- Richtlinie. Richtlinie (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

[16] ISO/IEC 29147:2018-10 (Ausgabedatum 2018-10), S. 14.

*Absatz 2–4: Frist für Behebung der Schwachstelle*

Das BACS verlangt von den Herstellern der von Schwachstellen betroffenen Hard- oder Software, eine Schwachstelle grundsätzlich innerhalb einer Frist von 90 Tagen zu beheben. Dies ist eine gängige Praxis in der Cybersicherheitsbranche.[17] Die Frist lässt den Herstellern genügend Zeit für die Analyse der Schwachstellen und für die Entwicklung und Umsetzung von Gegenmassnahmen, stellt andererseits aber auch sicher, dass die Schwachstellen nicht übermässig lange bestehen bleiben.

Abhängig von der Kritikalität und der Komplexität einer Schwachstelle kann die entsprechende Frist verkürzt werden. Es ist aber auch möglich, die angesetzte Frist im Bedarfsfall zu verlängern (z. B. infolge eines hohen Aufwands für Gegenmassnahmen oder eines erhöhten Koordinationsbedarfs).

*Absatz 5: Bekanntgabe der Schwachstelle vor Behebung oder Veröffentlichung*

Wenn dem BACS eine Schwachstelle bekannt ist, die für andere kritische Infrastrukturen eine akute Cyberbedrohung darstellt, informiert das BACS die Betreiberinnen, bevor die Schwachstelle veröffentlicht oder durch die Herstellerin der Hard- oder Software behoben wurde. Dieser Schritt ist wichtig, um die Betreiberinnen kritischer Infrastrukturen frühzeitig über potenzielle Sicherheitsrisiken zu informieren und ihnen die Möglichkeit zu geben, angemessene Massnahmen zum Schutz ihrer Systeme zu ergreifen. Durch den Austausch von Informationen über Schwachstellen können Betreiber kritischer Infrastrukturen proaktiv Massnahmen zur Risikominderung ergreifen, bevor die Schwachstellen öffentlich bekannt sind. Dies kann dazu beitragen, potenzielle Angriffe auf kritische Infrastrukturen zu verhindern oder abzuschwächen.

*Absatz 6: Ausnahmeregelung für das BAKOM*

Diese Bestimmung soll mögliche Kompetenzkonflikte und Doppelspurigkeiten zwischen dem BACS und dem BAKOM vermeiden. Das BAKOM übt die Marktaufsicht über das Anbieten, das Bereitstellen auf dem Markt, die Inbetriebnahme, das Erstellen und das Betreiben von Fernmeldeanlagen aus. Es führt dazu Marktkontrollen bei Wirtschaftsakteuren, in erster Linie beim Schweizer Hersteller oder, falls nicht vorhanden, beim Importeur, solcher Anlagen durch, prüft die betroffenen Anlagen und trifft die notwendigen Massnahmen, wenn die kontrollierten Anlagen die geltenden Vorschriften nicht einhalten (Art. 33 Fernmeldegesetz vom 30. April 1997[18]; FMG). Zu diesen Vorschriften gehören auch Cybersicherheitsanforderungen für gewisse Funkanlagen gemäss Art. 7 Abs. 3 Bst. d, e und f der Verordnung vom 25. November 2015[19] über Fernmeldeanlagen (FAV)[20].

---

17 Vgl. Leitlinie des deutschen Bundesamtes für Sicherheit in der Informationstechnik zum Coordinated Vulnerability Disclosure (CVD)-Prozess, Ziff. 3.3., S.10.

18 SR 784.10

19 SR 784.101.2

20 Die betroffenen Funkanlagen dürfen weder schädliche Wirkungen für das Netz oder seinen Betrieb haben noch Netzressourcen missbrauchen, wodurch eine unannehmbare Beeinträchtigung des Dienstes verursacht würde. Sie müssen Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre der Benutzerinnen und Benutzer sowie der Teilnehmerinnen und Teilnehmer verfügen. Sie müssen überdies bestimmte Funktionen zum Schutz vor Betrug unterstützen.

Da sich die Ziele des BACS und des BAKOM diesbezüglich überschneiden, ist die koordinierte Offenlegung nach Absatz 1 nicht durchführbar, wenn das BAKOM vor dem BACS anlässlich einer Kontrolle eines Wirtschaftsakteurs eine Nichteinhaltung der Cybersicherheitsanforderungen bei einer Funkanlage entdeckt. Der Wirtschaftsakteur hat im Verfahren der Marktkontrolle nach der Prüfung des BAKOM bereits vor dem ausländischen Fabrikanten Kenntnis, dass eine Schwachstelle bei den betroffenen Anlagen vorhanden ist. Es bedarf deshalb eines Koordinationsmechanismus, um die Verfahren des BAKOM und des BACS abzustimmen. Das BAKOM informiert entsprechend das BACS über Schwachstellen, welches gegebenenfalls die koordinierte Offenlegung der Schwachstellen nach Abs. 1 durchführt.

*Absatz 7: Information des BAKOM*

Das BAKOM benötigt umgehend die Informationen über die vom BACS entdeckten Schwachstellen in Fernmeldeanlagen. So kann einerseits sichergestellt werden, dass das BAKOM nicht gleichzeitig mit der koordinierten Offenlegung des BACS ein Verfahren eröffnet und andererseits wird es dem BAKOM mit diesen Informationen möglich sein, das weitere Vorgehen in einem bereits laufenden Verfahren im Rahmen seiner Marktaufsicht gegen einen Schweizer Hersteller oder einen Importeur zu bestimmen (siehe hierzu die vorstehenden Ausführungen zu Absatz 6).

Hat der vom BACS informierte Hersteller die Schwachstelle innert Frist beheben können, kann das BAKOM anschliessend prüfen, ob die Anpassungen des Herstellers auch bei den auf dem Markt erhältlichen Anlagen gemacht worden sind. Sollte die Schwachstelle nicht behoben worden sein, kann das BAKOM im Verfahren gegen den Importeur entsprechende Massnahmen verfügen.

## Art. 10 Unterstützung von Behörden

Diese Bestimmung stützt sich auf Art. 73*a* Abs. 2 Bst. c ISG.

Das BACS unterstützt als Kompetenzzentrum des Bundes für Cybersicherheit die zuständigen Behörden des Bundes und der Kantone bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit namentlich wie folgt:

- *Fachliche Expertise*: Es verfügt über spezialisierte Fachkräfte, welche die Behörden bei der Umsetzung der oben genannten Standards und Regulierungen zur Cybersicherheit beraten und unterstützen können.

- *Bereitstellung von technischer Unterstützung*: Es unterstützt die Behörden bei der Entwicklung und Umsetzung von Cybersicherheitsstandards und -regulierungen.

- *Koordination und Zusammenarbeit*: Es übernimmt die Koordination für die Erleichterung der Zusammenarbeit zwischen den verschiedenen Behörden und stellt sicher, dass die entwickelten Standards und Regulierungen in Bezug auf die Cybersicherheit kohärent und effektiv sind.

- *Informationsaustausch*: Es dient als Basis für den Austausch über die bewährten Praktiken und Informationen im Bereich Cybersicherheit zwischen den Behörden.

## 4. Abschnitt: Informationsaustausch

### Art. 11 Kommunikationssystem für den sicheren Informationsaustausch

Diese Bestimmung stützt sich auf Art. *73a* Abs. 1 und 2 Bst. e sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

Die Aufgabe des BACS betreffend sicheren Informationsaustausch wurde bis Ende 2023 in Art. 12 Abs. 1 Bst. b und i der aufgehobenen CyRV geregelt. Die OV-VBS enthält diesbezüglich keine spezifische Regelung.

*Absatz 1: Zugang zum sicheren Kommunikationssystem*

Angreifer verwenden oftmals die gleichen Methoden und Mittel, um bei möglichst vielen Opfern erfolgreiche Attacken durchzuführen. Wenn die Betroffenen anderen Organisationen und Behörden rasch ihre Erkenntnisse aus Cybervorfällen und Cyberbedrohungen mitteilen, kann deren Zahl deutlich verringert werden. Aus diesem Grund betreibt das BACS ein Kommunikationssystem für den sicheren Informationsaustausch zu Cybervorfällen und Cyberbedrohungen. Über dieses Kommunikationssystem kann das BACS den registrierten Behörden und Organisationen mit Sitz in der Schweiz rasch und effizient Informationen über Vorfälle und Bedrohungen mitteilen. Dies ermöglicht es den registrierten Organisationen und Behörden, schneller auf Bedrohungen zu reagieren und Gegenmassnahmen zu ergreifen. Des Weiteren trägt dieses Kommunikationssystem auch dazu bei, ein besseres Verständnis der Art und des Ausmasses von Cybervorfällen und Cyberbedrohungen zu entwickeln.

*Absatz 2: Verantwortung des BACS für die Sicherheit und den Datenschutz*

Das Kommunikationssystem für den sicheren Informationsaustausch ist ein Informationssystem des BACS. Dieses trägt die Verantwortung für die Sicherheit und gewährleistet die rechtmässige Bearbeitung der Daten.

### Art. 12 Informationssysteme für den automatischen Austausch

Diese Bestimmung stützt sich auf Art. *73a* Abs. 1 und 2 Bst. e sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

*Absatz 1: Automatischer Austausch von Informationen*

Die Zurverfügungstellung von Informationssystemen seitens des BACS für den automatischen Austausch von technischen Informationen ist ein sehr wichtiges Mittel zum Schutz der kritischen Infrastrukturen vor Cybervorfällen sowie -bedrohungen und ermöglicht es den Betreiberinnen von kritischen Infrastrukturen, stets über den aktuellsten Wissensstand zu verfügen. Das BACS nutzt diese geschützten Informationssysteme dazu, die kritischen Infrastrukturen frühzeitig über technische Indikatoren und

Angriffsmuster zu informieren, die der Öffentlichkeit noch nicht bekannt sind und vom BACS aus Sicherheitsgründen auch nicht veröffentlicht werden können. Technische Indikatoren zu Cybervorfällen oder -bedrohungen sind spezifische Anzeichen oder Hinweise auf potenzielle oder tatsächliche Bedrohungen im Bereich der Informationstechnologie und Cybersicherheit. Diese Indikatoren können verschiedene Formen annehmen, wie beispielsweise Malware-Signaturen, bei denen es sich um eindeutige Merkmale von schädlicher Software handelt, die darauf hinweisen, dass ein System infiziert ist oder einer Infektion ausgesetzt war. Auch Anomalien im Netzwerkverkehr gehören dazu. Hierbei handelt es sich beispielsweise um ungewöhnliche Muster im Datenverkehr, die auf eine mögliche Cyberbedrohung hindeuten können, wie ungewöhnlich hohe Datenübertragungsraten oder verdächtige Verbindungen zu bekannten schädlichen IP-Adressen. Ebenfalls können andere digitale Forensik-Indikatoren über diese Informationssysteme mit den Betreiberinnen kritischer Infrastrukturen automatisch ausgetauscht werden. Dies können verschiedene Arten von digitalen Spuren sein, die auf einen Cybervorfall oder eine Cyberbedrohung hindeuten, wie z.B. ungewöhnliche Dateiänderungen, verdächtige Logins oder unbefugte Zugriffsversuche. Betreiberinnen kritischer Infrastrukturen werden bei der Registrierung beim BACS entsprechend als solche erfasst, so dass die vorerwähnten technischen Informationen gezielt nur im Kreis der kritischen Infrastrukturen verteilt werden können. Alle erfassten Betreiberinnen kritischer Infrastrukturen werden einem oder mehreren Sektoren zugeteilt, damit auch ein sektorspezifischer Austausch erfolgen kann.

*Absatz 2: Verantwortung des BACS für die Sicherheit und den Datenschutz*

Analog zu den Bestimmungen in Artikel 12 Absatz 2 trägt das BACS auch für die Informationssysteme für den automatischen Informationsaustausch die Verantwortung für die Sicherheit und den Datenschutz.

## Art. 13 Registrierung

Diese Bestimmung stützt sich auf Art. *73a* Abs. 1 und 2 Bst. e sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

*Absatz 1: Registrierung für die Teilnahme am Informationsaustausch*

Interessierte Organisationen und Behörden müssen sich für die Teilnahme am Informationsaustausch registrieren und jeweils allfällige Änderungen der registrierten Angaben unverzüglich dem BACS melden.

*Absatz 2: Zu registrierende Angaben*

Die Registrierung muss mindestens folgende Informationen enthalten:

- *Firma, Name oder Bezeichnung und Adresse der Behörde oder Organisation (Bst. a)*: Damit die Behörden und Organisationen ordentlich identifiziert werden können, müssen sie anlässlich der Registrierung ihre Firma, ihren Namen oder ihre Bezeichnung und ihre Adresse mit folgenden Angaben angeben: Strasse, Hausnummer, Postleitzahl und Ortsname.

- *Kontaktangaben der gemeldeten Person (Bst. b):* Die Registrierung der Behörden oder Organisationen muss mindestens den Vornamen und den Familiennamen einer Kontaktperson enthalten. Des Weiteren ist die Telefonnummer sowie die E-Mail-Adresse und die Funktion der gemeldeten Person für das BACS anzugeben. Es können mehrere Kontaktpersonen registriert werden.

Einhergehend mit der Registrierung werden die Behörde oder Organisation über die Vorgaben für die Teilnahme am Informationsaustausch gemäss Art. 15 dieser Verordnung informiert, und ein Abschluss der Registrierung ist nur möglich, wenn die Kenntnisnahme der Vorgaben aktiv bestätigt wird.

Selbst für meldepflichtige Behörden und Organisationen ist die Registrierung für die Teilnahme am Informationsaustausch nicht zwingend. Eine frühzeitige Registrierung bedeutet für die Meldepflichtigen aber eine Zeitersparnis im Falle eines meldepflichtigen Cyberangriffs.

## Art. 14 Dienstleister

Diese Bestimmung stützt sich auf Art. *73a* Abs. 1 und 2 Bst. e sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

*Absatz 1: Anmeldung*

Um die Sicherheit und Integrität der kritischen Infrastrukturen in der Schweiz zu gewährleisten, haben die Betreiberinnen kritischer Infrastrukturen gemäss *Absatz 1* die Möglichkeit, ihre Dienstleister für die Cybersicherheit beim BACS zu melden, damit diese am Informationsaustausch teilnehmen können.

*Absatz 2: Zu registrierende Angaben*

Allfällig gemeldete Dienstleister von Betreiberinnen von kritischen Infrastrukturen müssen sich gemäss *Absatz 2* unter Angabe ihrer Firma oder dem Namen sowie

Kontaktangaben der gemeldeten Person registrieren (siehe hierzu sinngemäss die Ausführungen oben bei Artikel 13 Absatz 2).

## Art. 15 Übermittlung und Nutzung der Informationen

Diese Bestimmung stützt sich auf Art. 73*a* Abs. 1 und 2 Bst. e sowie Art. 74 Abs. 1 und 2 Bst. a ISG.

Der Informationsaustausch erfolgt freiwillig und basiert auf dem Vertrauen, dass die gelieferten Informationen zweckdienlich verwendet werden. Es ist deshalb entscheidend, dass die Informationslieferanten unter Berücksichtigung der gesetzlichen Vorgaben bestimmen können, wie mit der von ihnen geteilten Information umgegangen wird, und dass alle Teilnehmenden die Vorgaben für den Informationsaustausch kennen und einhalten.

*Absatz 1: Weitergabe der geteilten Informationen nur gemäss den Bestimmungen der Informationslieferanten*

Die Regelung, dass geteilte Informationen nur – soweit eine Weitergabe der Informationen nicht gesetzlich vorgesehen ist – gemäss den Bestimmungen der Informationslieferanten weitergegeben werden dürfen, ist wichtig, um sicherzustellen, dass die Informationen nicht unbefugt verbreitet oder missbraucht werden. Informationen über Cybervorfälle und -bedrohungen müssen vertraulich geteilt werden. Sie zeigen, welche Erkenntnisse über einen Vorfall vorliegen und welche Schutzmassnahmen identifiziert wurden. Angreifer könnten solche Informationen für ihre Zwecke nutzen. Zudem enthalten solche Informationen auch Angaben, die für die betroffene Behörde oder Organisation selbst sensibel sind, z.B. weil sie ihre Reputation gefährden können. Es ist darum wichtig, dass die Informationslieferanten grundsätzlich den Empfängerkreis selbst bestimmen können. In der Cybersicherheit hat sich zu diesem Zweck die Klassifizierung nach dem «Traffic Light Protocol» (TLP-Protokoll) durchgesetzt. Dieser vom «Forum of Incident Response and Security Teams (FIRST)» proklamierte Standard[21] unterscheidet folgende Vorgaben für die Weiterverbreitung von Informationen:

- TLP «clear» - keine Restriktion für die Verbreitung der Information.
- TLP «green» - die Empfänger dürfen Informationen weitergegeben, jedoch nicht auf öffentlichen Quellen publizieren.
- TLP «amber» - die Empfänger dürfen Informationen innerhalb ihrer Organisation[22] und mit ihren Partnern teilen, sofern dies nötig ist.

[21] Siehe hierzu Forum of Incident Response and Security Teams: Traffic Light Protocol (TLP), auf der Webseite Traffic Light Protocol (TLP) (first.org).

[22] Das TLP spezifiziert nicht, was unter «ihre Organisation» zu verstehen ist. Insbesondere bei Grossfirmen oder bei Verwaltungen kann das zu Unklarheiten führen. In der Bundesverwaltung wird das Protokoll so umgesetzt, dass unter «Organisation» eine Verwaltungseinheit, als z.B. ein Bundesamt gemeint ist.

- TLP «amber strict» - die Empfänger dürfen Informationen ausschliesslich innerhalb ihrer Organisation teilen.

- TLP «red» - die Information geht nur an das Individuum und darf nicht weitergegeben werden.

Die auf der Plattform des BACS geteilten Informationen sind gemäss dem TLP-Protokoll kategorisiert. So wird angezeigt, wie die Information weiterverbreitet werden darf. Diese Vorgaben sind für alle Empfänger verbindlich, ausser die Weitergabe der Informationen ist gesetzlich vorgesehen.

*Absatz 2:* *Entscheidung des BACS über die Veröffentlichung von Informationen*

Das BACS hat die Autorität, zu bestimmen, ob und wann zur Weitergabe freigegebene Informationen über Cyberbedrohungen und -angriffe öffentlich gemacht werden sollen und ist damit verantwortlich für die Entscheidung, welche dieser Informationen an wen weitergegeben werden dürfen. Es handelt sich hierbei um Informationen, die intern geprüft und bearbeitet werden. Dabei wird berücksichtigt, welche Informationen nützlich und relevant für die Öffentlichkeit oder bestimmte Zielgruppen sind und wie deren Verbreitung am besten über das vorhandene Kommunikationssystem bzw. den Informationssystemen erfolgen kann.

*Absatz 3:* *Gewährleistung des Schutzes der Informationen*

Den Informationsempfängern kommt die Verantwortung zu, Massnahmen zu ergreifen, um die Sicherheit und Vertraulichkeit der erhaltenen Informationen zu gewährleisten. Der Schutz dieser Informationen ist besonders wichtig, da sie sensibel sein können und ihre Offenlegung oder Kompromittierung negative Folgen haben könnten. Zum Beispiel könnte dies weitere Cyberangriffe begünstigen oder bereits bestehende Sicherheitsprobleme verschärfen.

*Absatz 4:* *Vorgaben für allfällige Dienstleister von Betreiberinnen kritischer Infrastrukturen*

Dienstleister, die für kritische Infrastrukturen tätig sind, und die von den Betreiberinnen der kritischen Infrastrukturen gemäss Artikel 14 dieser Verordnung angemeldet und registriert wurden, dürfen die Informationen, die sie erhalten, ausschliesslich für die spezifischen Tätigkeiten verwenden, die sie im Auftrag der kritischen Infrastruktur ausführen. Dies dient dazu, die Vertraulichkeit und den angemessenen Umgang mit sensiblen Informationen zu gewährleisten und das Risiko eines Missbrauchs oder eines unbefugten Zugriffs zu minimieren.

## 5. Abschnitt: Meldepflicht

### Art. 16 Ausnahmen von der Meldepflicht

Diese Bestimmung stützt sich auf Art. 74*c* ISG, wonach der Bundesrat Organisationen und Behörden von der Meldepflicht nach Art. 74*b* ISG ausnimmt, wenn durch

Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf die öffentliche Ordnung, die Sicherheit, das Wohlergehen der Bevölkerung oder das Funktionieren der Wirtschaft haben.

*Allgemeines:*

Sind Behörden oder Organisationen in mehreren Bereichen nach Art. 74*b* ISG meldepflichtig, so führt die Ausnahme in einem Bereich nicht dazu, dass sie von der Meldepflicht ausgenommen werden, sofern sie in einem oder mehreren anderen Bereichen noch meldepflichtig sind.

Es gilt auch zu beachten, dass es meldepflichtige Behörden und Organisationen gibt, für die keine Ausnahmen von der Meldepflicht gemäss den nachfolgend erläuterten Absätzen 1 und 2 bestehen. Zu diesen gehören:

- Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen (Art. 74*b* Abs. 1 Bst. i ISG);

- die Schweizerische Radio- und Fernsehgesellschaft (Art. 74*b* Abs. 1 Bst. j ISG); und

- Nachrichtenagenturen von nationaler Bedeutung (Art. 74*b* Abs. 1 Bst. k ISG).

*Absatz 1: Spezifische Schwellenwerte*

Es wurde darauf verzichtet, bereits auf Gesetzesstufe bereichsspezifische Ausnahmen zu definieren, damit der Bundesrat die Möglichkeit hat, auf Verordnungsstufe die festgelegten Schwellenwerte aufgrund von neuen Entwicklungen zeitnah anzupassen. Die Schwellenwerte wurden soweit möglich gemäss den spezifischen Herausforderungen des jeweiligen Bereichs definiert.

*Bst. a: Stellen nach Artikel 74b Absatz 1 Buchstaben b und c ISG*

Unter «*Stellen nach Art. 74b Abs. 1 Bst. b und c ISG»* versteht man:

- Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen (Art. 74*b* Abs. 1 Bst. b ISG), die für weniger als 1'000 Einwohnerinnen und Einwohner, gemessen an der ständigen Wohnbevölkerung, zuständig sind, sind von der Meldepflicht ausgenommen. Die in der Regel kleinen bis sehr kleinen Verwaltungen dieser Gemeinden sollen durch eine Meldepflicht nicht zusätzlich belastet werden. Der Schwellenwert von 1'000 Einwohnerinnen und Einwohnern der ständigen Wohnbevölkerung führt dazu, dass fast 40% der Gemeinden von der Meldepflicht ausgenommen sind. Davon wären gesamthaft rund 430'000 Einwohnerinnen und Einwohner betroffen.

- Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung, deren Tätigkeiten sich auf eine Gemeinde oder Organisation beschränkt, die für weniger als

1'000 Einwohnerinnen oder Einwohner, gemessen an der ständigen Wohnbevölkerung, zuständig ist, sind von der Meldepflicht ausgenommen.

Die Ausnahme gilt nicht für Anbieterinnen und Betreiberinnen von Diensten und Infrastrukturen, die der Ausübung der politischen Rechte dienen nach Art. 74*b* Abs. 1 Bst. s ISG. Diese sind auch dann meldepflichtig, wenn Sie Ihre Dienste und Infrastrukturen für weniger als 1'000 Einwohnerinnen und Einwohner anbieten.

*Bst. b: Unternehmen nach Artikel 74b Absatz 1 Buchstabe d ISG)*

Die hier für den Elektrizitätsbereich festgelegten Schwellenwerte orientieren sich an der Stromversorgungsverordnung vom 14. März 2008 (StromVV)[23], mit der die Empfehlungen des Minimalstandards zur Verbesserung der IKT-Resilienz[24] für gewisse Akteure der Elektrizitätsbranche für verbindlich erklärt werden sollen.[25] Darin wird vorgesehen, dass die Akteure bei der Umsetzung des Minimalstandards ein gewisses Niveau für den Schutz ihrer Anlagen vor Cyberbedrohungen erreichen müssen (Schutzniveau A, B oder C). Die Höhe des Schutzniveaus ist abhängig von der Grösse respektive dem Einfluss des Akteurs auf die Versorgungssicherheit und wird durch entsprechende Schwellenwerte bestimmt. Entsprechend sollen nur die Elektrizitätsunternehmen der beiden höchsten Schutzniveaus A und B der Meldepflicht unterstellt werden. Kleinere Akteure, welche die weniger hohen Anforderungen des Schutzniveaus C erfüllen müssen, werden von der Meldepflicht ausgenommen. Die Elektrizitätserzeuger und Elektrizitätsspeicherbetreiber sind wie die Netzbetreiber Akteure des Stromversorgungsrechts[26]. Sofern ein Unternehmen sowohl Anlagen zur Erzeugung als auch zur Speicherung von Elektrizität betreibt und diese Anlagen über dasselbe System fernsteuerbar sind, werden die Leistungen entsprechend zusammengerechnet. Dienstleister der Netzbetreiber, Elektrizitätserzeuger und Speicherbetreiber sind ebenfalls von der Ausnahmeregelung erfasst. Nicht zu den Dienstleistern gehören Herstellerinnen von Hard- oder Software gemäss Art. 74*b* Abs. 1 Bst. u ISG, für die es keine Ausnahmeregelung gibt.

Der in *Artikel 16 Absatz 1 Bst. b Ziffer 2 dieser Verordnung* für Betreiber von Gasleitungen definierte Schwellenwert von 400 GWh/Jahr wurde in Zusammenarbeit mit dem Verband der Schweizerischen Gasindustrie (VSG) festgelegt. Massgebend ist die gesamte über ihr Netz geleitete Energie (zu den Endverbrauchern oder zu anderen Netzen). Die Ausnahmeregelung betrifft nur Betreiber von Gasleitungen, deren

---

23 SR 734.71

24 Bundesamt für wirtschaftliche Landesversorgung, «Minimalstandard zur Verbesserung der IKT-Resilienz», Bern, 2018.

25 Das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) hat am 21. September 2023 die Vernehmlassung zu Teilrevisionen von verschiedenen Verordnungen im Energiebereich eröffnet. So ist vorgesehen, dass durch die Revision der Stromversorgungsverordnung (StromVV) der Schutz vor Cyberbedrohungen in der Stromversorgung gestärkt werden soll. Dazu wird der IKT-Minimalstandard für die wichtigsten Stromversorger – Netzbetreiber, Produzenten, und Speicherbetreiber – für verbindlich erklärt. Sie werden dazu einem bestimmten Schutzniveau (Schutzprofil) mit abgestuften Anforderungen zugeordnet, das sie erreichen müssen.

26 Zu den Elektrizitätserzeugern vgl. Art. 5 Abs. 2 des Stromversorgungsgesetzes vom 23. März 2007 (SR 734.7). Zu den Elektrizitätsspeicherbetreibern vgl. z.B. Art. 17*a* Abs. 1 StromVG oder Art. 8*a* Abs. 1 Bst. a Ziff. 3 StromVV.

Geschäftstätigkeit im Gasabsatz an Endverbraucher besteht (nicht von der Ausnahmebestimmung erfasst wäre daher bspw. die Transitgas AG).

Mit Art. 74*b* Abs. 1 Bst. d ISG werden neben den Elektrizitäts- und den Gasversorgungsunternehmen auch andere Energieunternehmen der Meldepflicht unterstellt, beispielsweise Betreiber von Rohrleitungen zur Beförderung von Erdöl, Fernheizwerke, Raffinerien oder Unternehmen in den Bereichen der Holzenergie und Kohle. Diese Unternehmen sind grundsätzlich meldepflichtig, ausser sie liegen unterhalb der in Art. 16 Abs. 2 Bst. b dieser Verordnung definierten Schwellenwerte. Unternehmen, die sowohl in der Elektrizitäts- oder Gasversorgung als auch in einem anderen Energiebereich (Erdöl, Fernwärme, etc.) tätig sind, können sich nur dann auf eine Ausnahmeregelung berufen, wenn sich der Cyberangriff bzw. dessen Auswirkungen auf diesen Energiebereich beschränkt.

Bereits nach Art. 74*b* Abs. 1 Bst. d ISG sind die Bewilligungsinhaber gemäss Kernenergiegesetz vom 21. März 2003[27] von der Meldepflicht ausgenommen. Dementsprechend erübrigt sich eine Regelung auf Verordnungsebene.

*Bst. c: Unternehmen nach Art. 74b Absatz 1 Buchstabe n ISG*

Unternehmen, die nach Art. 74*b* Absatz 1 Buchstabe n ISG definiert sind und keine spezifischen Sicherheitsmanagement- oder -programmvorgaben gemäss den genannten EU-Verordnungen erfüllen müssen, sind von der Pflicht ausgenommen, Cyberangriffe auf ihre Informatiksysteme an das BACS zu melden. Dies gilt für Unternehmen, die:

- nicht verpflichtet sind, ein Information Security Management System (ISMS) gemäss den Artikeln 2 und 4 und dem Anhang II der Verordnung (EU) 2023/203 vom 5. Oktober 2023 oder Artikel 2 und dem Anhang II der Verordnung (EU) 2022/1645 vom 14. Juli 2022 einzurichten. Diese sind auch von der Meldepflicht bei Cyberangriffen gegenüber dem BACS ausgenommen. Ein ISMS ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen, damit sie sicher bleiben. Es umfasst Personen, Prozesse und IT-Systeme durch Anwendung eines Risikomanagementprozesses. Die genannten Verordnungen der EU legen Standards und Anforderungen für die Einrichtung eines solchen Systems fest. Wenn ein Unternehmen nicht verpflichtet ist.

- welche nicht die Vorgaben nach Punkt 1.7 des Anhangs der Verordnung (EU) 2015/1998 umsetzen müssen: Diese Verordnung betrifft Sicherheitsvorschriften für die Zivilluftfahrt. Punkt 1.7 des Anhangs könnte spezifische Sicherheitsmassnahmen oder -standards enthalten, die in einem «Security Programme» umgesetzt werden müssen. Wenn das betreffende Unternehmen nicht verpflichtet ist, diese Vorgaben in seinem Sicherheitsprogramm umzusetzen – was wiederum auf Grundlage von Artikel 2, 12, 13 oder 14 der Verordnung (EG) 300/2008 erfolgt – dann ist es ebenfalls von der Meldepflicht bei Cyberangriffen befreit.

[27] SR 732.1

*Bst. d: Eisenbahnunternehmen nach Artikel 74b Absatz 1 Buchstabe m ISG*

Die Meldepflicht beschränkt sich auf die vom BAV beaufsichtigten Transportunternehmen mit Systemaufgaben im öffentlichen Interesse, deren sicherer und zuverlässiger Betrieb für das Wohlergehen der Bevölkerung und das Funktionieren der Wirtschaft unerlässlich ist. Dementsprechend werden die übrigen Unternehmen von der Meldepflicht ausgenommen.

*Bst. e: Anbieterinnen und Betreiberinnen nach Artikel 74b Absatz 1 Buchstabe t ISG*

Anbieterinnen und Betreiberinnen von Cloudcomputing und Suchmaschinen sowie Rechenzentren, die einen Sitz in der Schweiz haben, sind nur dann meldepflichtig, wenn sie ihre Leistungen teilweise oder vollumfänglich für Dritte und gegen Entgelt erbringen. Durch das neu eingeführte Kriterium der gewerblichen Leistungserbringung fallen auch Rechenzentren nicht unter die Meldepflicht, die ihre Leistung ausschliesslich für den Eigenbedarf erbringen.

Ebenso unterliegen alle digitalen Sicherheitsdienste und alle digitalen Vertrauensdienste, die Dritten angeboten werden, unabhängig von ihrem Umsatz oder ihrer Klientel, der Meldepflicht für Cyberangriffe (ohne einen mittleren Schwellenwert). Dagegen unterliegen Dienste, die eine Person ausschliesslich für sich selbst entwickelt und nutzt, nicht der Meldepflicht.

*Absatz 2: Sektorenübergreifende Schwellenwerte*

Für die Meldepflicht von Unternehmen wurde als generelle Ausnahme auf den Schwellenwert der Unternehmensklasse «kleine Unternehmen» gemäss der Empfehlung der EU-Kommission abgestellt.[28] Demnach sind meldepflichtige Behörden und Organisationen nach Art. 74*b* ISG von der Meldepflicht ausgenommen, wenn sie weniger als 50 Personen beschäftigen und ihr Jahresumsatz bzw. ihre Jahresbilanz CHF 10 Mio. nicht übersteigt. Es wurde darauf verzichtet, eine Umrechnung von Euro in Schweizerfranken vorzunehmen, da die europäische Regelung auch für wirtschaftlich schwächere EU-Ländern gilt, in denen der Jahresumsatz bzw. die Jahresbilanz von Euro 10 Mio. schwieriger zu erreichen sein dürfte.

Die Ausnahme nach Absatz 2 gilt nur für meldepflichtige Unternehmen, für die keine spezifischen Schwellenwerte nach Absatz 1 definiert wurden. Hierzu gehören:

- Gesundheitseinrichtungen, die auf der kantonalen Spitalliste nach Art. 39 Abs. 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[29] über die Krankenversicherung aufgeführt sind (Art. 74*b* Abs. 1 Bst. f ISG);

- medizinische Laboratorien mit einer Bewilligung nach Art. 16 Abs. 1 des Epidemiengesetzes vom 28. September 2012[30] (Art. 74*b* Abs. 1 Bst. g ISG);

---

28 EU-Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG).
29 SR 832.10
30 SR 818.101

- Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[31] haben (Art. 74*b* Abs. 1 Bst. h ISG);

- Anbieterinnen von Postdiensten, die gemäss Art. 4 Abs. 1 des Postgesetzes vom 17. Dezember 2010[32] bei der Postkommission registriert sind (Art. 74*b* Abs. 1 Bst. l ISG); und

- Unternehmen, welche die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde (Art. 74*b* Abs. 1 Bst. p ISG).

Es gilt an dieser Stelle hervorzuheben, dass die in Absatz 2 aufgeführte Ausnahme nicht für Bundes-, Kantons- und Gemeindebehörden (Art. 74*b* Abs. 1 Bst. b ISG) und Hochschulen (Art. 74*b* Abs. 1 Bst. a ISG) gilt.

### Art. 17 Dokumentationspflicht bei Gesuchen um Auskunft über die Unterstellung unter die Meldepflicht

Diese Bestimmung stützt sich auf Art. 74*a* Abs. 2 ISG.

Da die Meldepflicht gemäss der Aufzählung in Art. 74*b* Abs. 1 ISG sehr viele verschiedene Bereiche erfasst und es zahlreiche Behörden und Organisationen gibt, die gemäss Art. 74*c* ISG und Artikel 16 dieser Verordnung von der Meldepflicht ausgenommen sind, ist zu erwarten, dass trotz dieser ausführlichen Regelungen bei gewissen Behörden und Organisationen Unklarheiten darüber bestehen, ob sie der Meldepflicht unterstellt sind oder nicht. Interessierte Behörden und Organisationen können daher beim BACS vorstellig werden und darum nachsuchen, dass es Auskunft über das Bestehen einer Meldepflicht nach Art. 74*b* ISG oder einer Ausnahme von der Meldepflicht nach Art. 74*c* ISG erteilt.

Damit das BACS diese Auskunftsgesuche behandeln kann, sieht der vorliegende *Artikel 17* vor, dass Behörden und Organisationen dem BACS alle erforderlichen Unterlagen zur Verfügung stellen müssen, damit das Amt darüber Auskunft geben kann, ob diese Einrichtungen einer gesetzlichen Meldepflicht unterliegen. Diese Anforderung stellt sicher, dass das BACS seine Aufgaben im Bereich der Cybersicherheit effektiv wahrnehmen kann. Da die Auskunft des BACS quasi eine Momentaufnahme darstellt, die auf den zum Zeitpunkt ihrer Erstellung vorliegenden Sachverhalten basiert, liegt es in der Verantwortung der betroffenen Behörde oder Organisation, bei einer wesentlichen Änderung der relevanten Tatsachen oder Umstände unverzüglich ihrer Meldepflicht nachzukommen oder bei Unsicherheit beim BACS ein Auskunftsgesuch zu stellen.

31 SR 812.21
32 SR 783.0

## Art. 18 Zu meldende Cyberangriffe

Diese Bestimmung stützt sich auf Art. 74*d* ISG.

*Allgemeines*

Die Umschreibung der zu meldenden Cyberangriffe ist in Art. 74*d* Bst. a–d ISG festgehalten. Cyberangriffe sind grundsätzlich dann meldepflichtig, wenn sie zum Zweck der Frühwarnung und Beurteilung der Bedrohungslage für das BACS besonders relevant sind. Die Kriterien zur Bestimmung der meldepflichtigen Angriffe wurden so gewählt, dass sie für die Behörden und Organisationen möglichst direkt erkennbar sind. Sie werden in diesem Artikel auf Verordnungsstufe weiter präzisiert.

*Absatz 1: Gefährdung der Funktionsfähigkeit der kritischen Infrastruktur (Art. 74d Bst. a ISG)*

Die Funktionsfähigkeit einer kritischen Infrastruktur kann durch einen Cyberangriff gefährdet sein, wenn die IT-Systeme, Netzwerke oder Steuerungssysteme, die für den Betrieb der Infrastruktur wesentlich sind, dergestalt kompromittiert werden, dass es zu Systemunterbrüchen für Mitarbeitende und Dritte führt (Art. 18 Abs. 1 Bst. a dieser Verordnung) oder die betroffene Organisation oder Behörde ihre Tätigkeiten nur noch mit Hilfe von Notfallplänen aufrechterhalten kann (Art. 18 Abs. 1 Bst. b dieser Verordnung). Ein Systemunterbruch liegt dann vor, wenn Mitarbeitende oder Dritte für ihre Tätigkeit wichtige Arbeitsschritte nicht mehr ausführen können, weil die dazu nötigen Informatikmittel nicht mehr verfügbar sind. Als Notfallpläne gelten alle technischen oder organisatorischen Massnahmen, die ergriffen werden müssen, wenn die üblicherweise verwendeten Informatikmittel kurzfristig und ungeplant nicht mehr verfügbar sind.

*Absatz 2: Manipulation oder Abfluss von Informationen (Art. 74d Bst. b ISG)*

Von einem meldepflichtigen Cyberangriff infolge Manipulation oder einem Abfluss von Informationen geht man namentlich aus, wenn die Angreifer in der Lage sind unbefugten Zugriff auf sensible Daten der betroffenen Organisationen und Behörden zu erlangen und diese zu verändern, zu verschlüsseln, zu stehlen, zu löschen, Unbefugten offenzulegen oder zugänglich zu machen. So können durch einen Cyberangriff Daten durch Unbefugte dergestalt manipuliert werden, dass diese gemäss Art. 18 Abs. 2 Bst. a dieser Verordnung geschäftsrelevante Informationen in Systeme einspeisen, welche aufgrund ihrer Veränderung oder Offenlegung zu Fehlern in Geschäftsprozessen, zu falschen Entscheidungen oder sogar zu Sicherheitsrisiken führen. Möglich ist aber auch gemäss Art. 18 Abs. 2 Bst. b dieser Verordnung, dass durch die Manipulation oder den Abfluss von Informationen die Datensicherheit von Personendaten gemäss Art. 5 Bst. h i.V.m. Art. 24 DSG verletzt wurde.

*Absatz 3: Über einen längeren Zeitraum unentdeckter Cyberangriff (Art. 74d Bst. c ISG)*

Meldepflichtig sind auch Cyberangriffe, die über einen längeren Zeitraum unentdeckt bleiben und Anzeichen aufweisen, dass diese zur Vorbereitung weiterer Angriffe ausgeführt wurden. In Art. 18 Abs. 3 dieser Verordnung wird festgehalten, dass man

dann von einem längeren Zeitraum i.S.v. Art. 74*d* Bst. c ISG ausgeht, wenn nach der Entdeckung festgestellt wird, dass der Cyberangriff bereits vor mehr als 90 Tagen erfolgt ist (z.B. durch die Auswertung von Logdaten). Solche Cyberangriffe stellen eine ernsthafte Bedrohung für kritische Infrastrukturen dar. Sie werden häufig auch als «Advanced Persistent Threats» (APTs) bezeichnet. Sie sind in der Regel hochentwickelt, zielgerichtet und schwer zu erkennen. Aus diesem Grund sind sie als Warnung für andere Betreiberinnen und Betreiber kritischer Infrastrukturen von besonderer Relevanz. Bei dieser Art von Angriffen kann Spionage (z. B. Behörden- oder Industriespionage) nicht ausgeschlossen werden. Die Angriffe sind oft sehr komplex und werden von erfahrenen Angreifern durchgeführt, die fortgeschrittene Techniken und Werkzeuge einsetzen, um sich im System zu verstecken und ihre Aktivitäten zu verschleiern. In der Regel wird auf ausgewählte Organisationen, Branchen oder Behörden abgezielt. Es ist auch denkbar, dass die Angreifer schrittweise vorgehen, um Zugriffsberechtigungen zu erweitern und weitere Schwachstellen auszunutzen. Wenn Anzeichen dafür bestehen, dass ein Cyberangriff zur Vorbereitung für weitere Angriffe ausgeführt wurde, ist es wahrscheinlich, dass die Angreifer bereits Zugang zu kritischen Systemen oder Daten haben und diese für zukünftige Attacken nutzen können.

*Absatz 4: Mit Erpressung, Drohung oder Nötigung verbundener Cyberangriff (Art. 74d Bst. d ISG)*

Dieser Absatz statuiert, dass bei strafrechtlich relevanten Begleitumständen ein Cyberangriff immer dann zu melden ist, wenn sich diese strafbaren Handlungen gegen die meldepflichtige Behörde oder Organisation, gegen aktuelle oder ehemalige Verantwortliche oder gegen aktuelle oder ehemalige Mitarbeitende oder für die meldepflichtige Behörde oder Organisation tätige Personen richten. Viele Cyberkriminelle versuchen, über die Androhung oder Durchführung von Angriffen die Betreiberinnen kritischer Infrastrukturen, deren Kundinnen und Kunden oder einzelne Mitarbeitende zu erpressen (z. B. über die Verschlüsselung mittels Ransomware, der Androhung von Angriffen auf die Verfügbarkeit mittels Distributed-Denial-of-Service-Attacken [DDoS-Attacken] oder der Androhung der Veröffentlichung von sensiblen Informationen wie Personendaten oder Unternehmensgeheimnisse). Cyberangriffe mit strafrechtlich relevanten Begleitumständen sind meldepflichtig, wenn die Erpressung, Drohung oder Nötigung einen Bezug zur meldepflichtigen Organisation oder Behörde hat und sich auf deren Geschäfts- oder Verwaltungstätigkeit negativ auswirken kann. Es handelt sich dabei um schwerwiegende Auswirkungen, einschliesslich finanzieller Verluste, Rufschädigung oder rechtlicher Konsequenzen. Die Meldung solcher Angriffe ist wichtig, damit das BACS einschätzen kann, wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist.

## Art. 19 Inhalt der Meldung

Diese Bestimmung stützt sich auf Art. 74*e* Abs. 2 ISG.

*Allgemeines:*

Beim Verfassen dieser Ausführungsbestimmung hat man sich in weiten Teilen an der Terminologie und dem Inhalt des per 1. September 2020 eingeführten Formulars

der FINMA betreffend die «Meldepflicht von Cyber-Attacken» orientiert.[33] Da das BACS im Gegensatz zur FINMA keine Aufsichtsfunktion hat, wurden gewisse Angaben nicht übernommen, da sie für die Zwecke der Meldepflicht an das BACS nicht massgeblich sind. So sind zum Beispiel bei der Meldung an das BACS weder Angaben zu den kritischen Funktionen oder den Kommunikationsmassnahmen zu machen, da diese Informationen keinen Mehrwert für die Einschätzung des Cyberangriffs bzw. der Warnung allfälliger weiterer Betroffener bieten würden. Im Übrigen wurden für die Analyse von Cyberangriffen auch wichtige Hinweise aus dem Formular für IT-Sicherheitsvorfälle des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) übernommen.[34] Das Meldeformular für Datensicherheitsverletzungen,[35] deren Meldungen an den EDÖB erfolgen, wurde für die Meldepflicht bei Cyberangriffen ebenfalls als Orientierungshilfe verwendet.

Art. 74*e* Abs. 2 ISG nennt den Inhalt der Meldung, d.h. die wesentlichen Informationen, die zur Erfüllung der Meldepflicht notwendig sind. Der konkrete Umfang und Inhalt der zu meldenden Informationen wird in der vorliegenden Ausführungsbestimmung präzisiert und vom BACS in einem Formular auf seinem Kommunikationssystem übernommen. In diesem Formular wird zudem detailliert umschreiben, was unter den jeweils zu meldenden Informationen zu verstehen ist.

Im Übrigen wird an dieser Stelle nochmals darauf hingewiesen, dass zur Erfüllung der Meldepflicht gegenüber dem BACS keine Angaben gemacht werden müssen, die allfällige Berufs- oder Geschäftsgeheimnisse betreffen und diese verletzen oder einer strafrechtlichen Selbstbelastung gleichkommen (vgl. Art. 74*e* Abs. 4 ISG).

*Absatz 1: Informationen zur Art und Ausführung des Cyberangriffs*

Die Meldung gemäss *Absatz 1* umfasst folgende Informationen über die Art und Ausführung des Cyberangriffs:

- *Datum und Uhrzeit der Feststellung des Angriffs (Bst. a):* In der Meldung ist der Zeitpunkt der Entdeckung des Cyberangriffs mit Angabe des Datums sowie Uhrzeit aufzuführen.

- *Datum und Uhrzeit des Angriffs (Bst. b):* In der Meldung sind auch das Datum und die Uhrzeit des Angriffs anzugeben. Falls dieser nicht bekannt ist, kann auch der vermutete Zeitpunkt des Cyberangriffs angegeben werden.

- *Art des Angriffs (Bst. c):* Zur Art und Ausführung des Cyberangriffs werden im Meldeformular die wichtigsten Angriffsarten (z.B. DDoS, Unautorisierter Zugriff, Schadsoftware, Missbrauch / unsachgemässe Benutzung von Technologiein-

[33] Vgl. FINMA-Aufsichtsmitteilung 05/2020 vom 7. Mai 2020, welche sich auf Art. 29 Abs. 2 des Bundesgesetzes über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz, FINMAG; SR 956.1) stützt und durch die FINMA im Rundschreiben 2023/1 präzisiert wurde (FINMA-RS 2023/1 Rz 68).

[34] Vgl. das Meldeformular für IT-sicherheitsrelevante Ereignisse auf dem Melde- und Informationsportal des deutschen Bundesamts für Sicherheit in der Informationstechnik.

[35] Vgl. den Online-Dienst zur Meldung von Datensicherheitsverletzungen (Art. 24 DSG).

frastruktur usw.) zur Auswahl vorgegeben. Zusätzlich bietet das Meldeformular die Möglichkeit, den Cyberangriff in einem Freitextfeld zu beschreiben.

- *Angriffsmethode (Bst. d):* Zu den häufigsten Angriffsmethoden, in der Fachsprache Angriffsvektoren genannt, gehören beispielsweise Phishing-Angriffe, Ausnutzung von Schwachstellen, Überlastungsangriffe auf Server, Identitätsdiebstahl, etc. Im Meldeformular werden die häufigsten Angriffsmethoden/-vektoren angegeben, wobei Mehrfachnennungen möglich sind und auch nicht aufgezählte Methoden bzw. Vektoren genannt werden können.

- *Angaben zum Verursacher (Bst. e):* Die Identifizierung der Verursacher eines Cyberangriffs kann eine komplexe und herausfordernde Aufgabe sein, da Angreifer oft versuchen, ihre Spuren zu verschleiern und anonym zu bleiben. Dennoch gibt es verschiedene Arten von Informationen, die zur Identifizierung der Verursacher eines Cyberangriffs beitragen können, wie beispielsweise IP-Adressen, DNS-Records, URL von verdächtigen Seiten, hash-Werte von Malware, Virensignaturen, Anomalien im Netzwerkverkehr oder verdächtiges Verhalten von Software. Sind solche Informationen vorhanden, sind diese der Meldung anzufügen.

*Absatz 2: Angaben, ob eine Erpressung, Drohung oder Nötigung im Zusammenhang mit dem Cyberangriff erfolgt ist und ob Strafanzeige erstattet wurde*

Die Offenlegung von Erpressungsversuchen oder Drohungen im Zusammenhang mit einem Cyberangriff kann dazu beitragen, andere potenzielle Opfer zu warnen und Massnahmen zur Prävention ähnlicher Vorfälle zu ergreifen. Da eine Erpressung, Drohung oder Nötigung im Zusammenhang mit einem Cyberangriff strafrechtliche Konsequenzen haben kann, kommt es vor, dass meldepflichtige Behörden und Organisationen Strafanzeige erstatten. Die Angabe, ob eine Strafanzeige erstattet wurde, hilft dem BACS dabei, angemessen auf den Vorfall zu reagieren.

*Absatz 3: Informationen zu den Auswirkungen des Cyberangriffs*

Die gemäss *Absatz 3 Buchstaben a–c* zu machenden Angaben helfen dem BACS bei einer Erstbeurteilung der Auswirkungen des Cyberangriffs und in welcher Hinsicht Informatikmittel bzw. Daten durch den Cyberangriff beeinträchtigt sind.

- *Nennung der betroffenen Einheiten der Organisation oder Behörde (Bst. a):* Die Nennung der vom Cyberangriff betroffenen Einheit hilft dem BACS insbesondere bei Grossunternehmen, Konglomeraten und Konzernen mit zahlreichen Tätigkeitsbereichen bei der Beurteilung, ob die Informatikmittel bzw. Daten der kritischen Infrastruktur betroffen sind.

- *Schweregrad der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit der eigenen Informationen und der Informationen von Dritten (Bst. b):* Die meldepflichtige Behörde und Organisation hat abzuschätzen, welche Schutzziele (Verfügbarkeit, Integrität und Vertraulichkeit) durch den Cyberangriff auf die Informatikmittel wie stark betroffen sind. Je nach Einschätzung der Auswirkungen des Cyberangriffs wird die Beeinträchtigung der Schutzziele entsprechend einem Schweregrad mit den Prädikaten «gering, mittel, hoch oder

schwerwiegend» analog dem Meldeformular der FINMA zugeordnet.[36] Gestützt auf diese Erstbeurteilung der Auswirkungen und die Zuordnung der Schweregrade kann unter Umständen eruiert werden, ob sich bei den Auswirkungen ein Trend abzeichnet. Diese Information ist insbesondere dann wertvoll, wenn es Anzeichen für eine Verschlimmerung gibt. Des Weiteren hilft diese Einteilung auch bei der Entscheidfindung im Falle einer beantragten Hilfeleistung des BACS für die konkrete Vorgehensweise bei der Vorfallbewältigung.

– *Wirkung des Cyberangriffs auf die Funktionsfähigkeit der betroffenen Einheiten der Organisation oder Behörde (Bst. c):* Die Angaben zur Wirkung des Cyberangriffs auf die Funktionsfähigkeit der Organisation oder Behörde müssen darüber informieren, wie beispielsweise der Zugang zu Systemen und Daten, die Verfügbarkeit von Diensten für Kunden oder Bürgerinnen, interne Abläufe sowie Prozesse, die Verfügbarkeit von Strom- und Wasserversorgungssystemen, Gesundheitsdiensten oder andere kritische Infrastrukturen betroffen sind. Die meldepflichtige Organisation oder Behörde kann sich auch zu Angaben über den Zeitrahmen und Dauer der Auswirkungen des Cyberangriffs äussern und kundtun, wie lange die Auswirkungen des Cyberangriffs voraussichtlich anhalten werden.

*Absatz 4: Informationen zur meldepflichtigen Behörde oder Organisation*

Sofern die meldepflichtige Behörde oder Organisation nicht bereits für die Teilnahme am Informationsaustausch registriert und zum Zeitpunkt der Meldungserstattung keine Registrierung möglich ist (z. B. infolge Ausfalls der Informatikmittel) oder seitens der meldepflichtigen Behörde oder Organisation nicht gemacht werden will, muss die Meldung des Cyberangriffs gemäss *Absatz 4* zusätzlich folgende Informationen zur meldepflichtigen Behörde oder Organisation enthalten:

– *Firma, Name oder Bezeichnung und Adresse der meldepflichtigen Behörde oder Organisation (Bst. a)*: Zur ordentlichen Identifikation der meldepflichtigen Behörden und Organisationen müssen diese ihre Firma, ihren Namen oder ihre Bezeichnung sowie ihre Adresse mit folgenden Angaben: Strasse, Hausnummer, Postleitzahl und Ortsnamen angeben.

– *Kontaktangaben der meldenden Person (Bst. b):* Die Meldung hat mindestens einen Vornamen sowie den Familiennamen der gemeldeten Person zu enthalten. Des Weiteren sind die Telefonnummer sowie die E-Mail-Adresse der meldenden Person anzugeben, da diese die Kontaktperson für das BACS ist. Organisationen oder Behörden können mehrere Kontaktpersonen anmelden.

## Art. 20 Übermittlung der Meldung

Diese Bestimmung stützt sich auf Art. 74*f* ISG.

[36] Vgl. hierzu den Anhang 1 der FINMA-Aufsichtsmitteilung 05/2020 vom 7. Mai 2020, S. 7.

Das BACS bestätigt gemäss *Artikel 20* den Eingang der Meldung gegenüber der meldepflichtigen Behörde und Organisation umgehend, falls diese nicht über das Kommunikationssystem des BACS erfolgt. Erfolgt die Meldung beispielsweise mittels E-Mail, informiert das BACS allfällige gemäss Artikel 13 Absatz 2 Buchstabe b dieser Verordnung vorgängig registrierte Kontaktpersonen der meldepflichtigen Behörden und Organisationen. Mit dieser Rückmeldung soll sichergestellt werden, dass die meldepflichtige Behörde oder Organisation dem BACS mitteilen können, dass es sich um eine Falschmeldung handelt (z. B. «Scherzmeldung» durch Drittpersonen).

## Art. 21 Frist zur Erfassung der Meldung

Diese Bestimmung stützt sich auf Art. 74*e* Abs. 1 und 3 ISG.

*Allgemeines:*

Die meldepflichtigen Behörden und Organisationen müssen Cyberangriffe unverzüglich nach Bekanntwerden melden, denn es gilt der Grundsatz: «Schnelligkeit vor Vollständigkeit», da das BACS auf eine unverzügliche Meldung von meldepflichtigen Cyberangriffen angewiesen ist, um jeweils seinem gesetzlichen Auftrag der Frühwarnung gerecht zu werden.

*Absatz 1: Ergänzung oder Änderung der Meldung*

Da es insbesondere für die Frühwarnung und die Prävention entscheidend ist, dass Cyberangriffe unmittelbar nach ihrer Entdeckung von den meldepflichtigen Behörden und Organisationen gemeldet werden, schreibt Art. 74*e* Abs. 1 ISG eine Meldefrist von 24 Stunden vor. Der Fristenlauf beginnt nach der Entdeckung des Cyberangriffs. Innerhalb der Frist müssen die bis zu diesem Zeitpunkt bekannten Informationen gemeldet werden. Bei Cyberangriffen ist sehr oft während längerer Zeit unklar, wie gravierend der Angriff ist und was genau passiert ist. Falls die vom BACS gemäss Art. 19 dieser Verordnung verlangten Angaben zum Zeitpunkt der Meldung nur unvollständig vorliegen, können die Betroffenen die Meldung mit den fehlenden Angaben aufgrund neuer Erkenntnisse sowie ausreichendem Kenntnisstand ergänzen oder bestätigen, dass diese Informationen nicht vorhanden sind. Diese Nachmeldung muss dem BACS innerhalb einer Frist von 14 Tagen ab dem Zeitpunkt der Meldung des Cyberangriffs übermittelt werden. Beide Fristen sind nicht verlängerbar, da es sich um gesetzliche Fristen handelt (vgl. Art. 22 Abs. 1 VwVG).

*Absatz 2: Aufforderung des BACS*

Wenn die meldepflichtige Behörde oder Organisation nicht fristgerecht innerhalb der vorgeschriebenen 14 Tage die verlangten Informationen über den Cyberangriff meldet, so hat das BACS eine Aufforderung an die meldepflichtige Behörde oder Organisation zu erlassen. In dieser Aufforderung verlangt das BACS von der meldepflichtigen Behörde oder Organisation, die Meldung umgehend zu ergänzen oder zu bestätigen, dass diese Informationen nicht vorhanden sind.

### 6. Abschnitt: Schlussbestimmungen

### Art. 23 Inkrafttreten

Die Verordnung tritt gleichzeitig mit dem revidierten ISG am 1. Januar 2025 in Kraft.

# 3 Änderung anderer Erlasse

### 1. Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

### Art. 15*a* Abs. 2 Bst. f OV-VBS

Da in Artikel 7 dieser Verordnung die Aufgaben des Computer Emergency Response Teams (CERT) des BACS näher umschreiben werden, wird der bisherige Artikel 15*a* Absatz 2 Buchstabe f OV-VBS entsprechend gekürzt, damit keine Doppelspurigkeit besteht.

### Art. 15*a* Abs. 2 Bst. h OV-VBS

In Artikel 15*a* Absatz 2 Buchstabe h OV-VBS wird neu aufgeführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien vertritt. Diese Nennung ist wichtig, da Cybervorfälle und Cyberbedrohungen internationale Phänomene sind. Angreifer benutzen die gleichen Technologien und Methoden in vielen Ländern gleichzeitig. Der nationale und internationale Austausch zwischen Fachstellen ist deshalb für den Schutz vor Cybervorfällen und Cyberbedrohungen unerlässlich. Das BACS tauscht diesbezügliche aktiv Informationen mit inländischen und internationalen Stellen aus, die ähnliche Aufgaben wie das BACS wahrnehmen. Dieser Informationsaustausch dient dazu, relevante Erkenntnisse und Daten über aktuelle Bedrohungen zu teilen und gemeinsame Massnahmen zur Bewältigung von Cybervorfällen und Cyberbedrohungen zu koordinieren. Damit hat das BACS mit seinem CERT im Verhältnis zu den EU-Staaten den Stellenrang eines nationalen «Computer Security Incident Response Teams (CSIRT)», wie es die NIS-2-Richtlinie der EU für alle EU-Mitgliedstaaten vorschreibt.[37] Darüber hinaus vertritt das BACS die Schweiz in internationalen Fachgremien, die sich mit der technischen Analyse von Cybervorfällen und Cyberbedrohungen sowie mit der technischen Vorfallbewältigung befassen. Das bedeutet, dass das BACS an internationalen Foren und Arbeitsgruppen teilnimmt, um sein Fachwissen und seine Erfahrung im Bereich der Cybersicherheit einzubringen und von den Erkenntnissen anderer Länder zu profitieren. Durch den Austausch von Informationen und die Teilnahme an internationalen Fachgremien trägt das BACS dazu bei, dass die Schweiz auf dem neuesten Stand der Entwicklungen im Bereich der Cybersicherheit bleibt und von Best Practices aus anderen Ländern profitiert. Dies stärkt die Fä-

[37] Richtlinie (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

higkeit des BACS, angemessen auf Cybervorfälle und Cyberbedrohungen zu reagieren und zur globalen Sicherheit beizutragen. All diese Aufgaben erfordern einen Informationsaustausch mit inländischen, ausländischen sowie internationalen Stellen, dessen gesetzliche Grundlagen in Art. 73*d* Abs. 1 und Art. 76, 76*a* und 77 ISG zu finden sind.

## 2. Verordnung über den Datenschutz vom 31. August 2022

### Art. 41 Abs. 1 DSV

Da das Parlament am 29. September 2023 eine Änderung des ISG verabschiedet hat, mit welcher eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen auf den 1. Januar 2025 eingeführt wird, muss Art. 41 Abs. 1 der Verordnung über den Datenschutz vom 31. August 2022 aufgehoben werden.